CSOPORTKÓDOK ELŐÁLLÍTÁSA A WANG—2200/C SZÁMÍTÓGÉPEN

PUSKÁS ALBERT

Az információelmélet az információk (hírek: betűk, számok, jelek véges sorozatai; a továbbiakban közleményszavak) tárolásával és továbbításának leggazdaságosabb és legmegbízhatóbb módszereivel foglalkozó tudományág.

A legegyszerűbb hírközlő rendszer alapsémája: *forrás→csatorna→vevő*. Megkülönböztetünk zajmentes és zajos csatornákat. Ha a csatorna zajos, akkor problémát jelenthet a vevő oldalán vett jelsorozatok biztonsága. Ezért igen fontosak azok az eljárások, melyek a forrás által kibocsátandó közleményszavakat átalakítják (kölcsönösen és egyértelműen) olyan kódszavakká, melyek kibocsátása, továbbítása és vétele után nagyobb biztonsággal következtethetünk az eredeti közleményszóra. Az ilyen eljárásokat kódolási eljárásoknak (röviden kódolásnak) nevezzük. Kódolás tehát az információ átalakítása adott eljárás szerint biztonságos továbbítás céljából. Ezekután a hírközlő rendszer sémája: *forrás→kódoló→csatorna→dekódoló→vevő* [3].

A dolgozat egy részében összefoglaljuk azokat az ismert definíciókat, tételeket, melyek a dolgozat más részében közölt számítógépes programok megértéséhez, felhasználásához, a közölt programok tulajdonságaihoz szükségesek [1], [2].

Digitális információ kódolásról és dekódolásról beszélünk akkor, ha a közlemény- és kódszavak számjegyek. E dolgozatban a digitális információk kódolásával foglalkozunk. Legegyszerűbb digitális kódolás a bináris kódolás.

A továbbiakban jelölje Z a 0, 1, 2, ..., $z-1$ z alapú számrendszer számjegyeiből álló halmazt.

Definíció. *Egy digitális* — a Z halmaz elemeire felírt — *közlemény* (m, n) *kódja egy*

$$K: z^m \to z^n$$

kódolási sémából, és egy

$$D: z^n \to z^m$$

dekódolási sémából áll.

Ha Z a $\{0, 1\}$ halmaz, akkor bináris kódolásról beszélünk. Ekkor mind a közlemény-, mind a kód-szavak 0 és 1 jegyek sorozataiból állnak. Pl. egy (2,3) kódolás ekkor a következő kódolási sémát jelentheti:

$$00 \to 000$$
$$01 \to 011$$
$$10 \to 101$$
$$11 \to 110$$

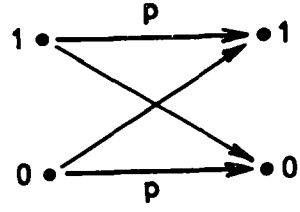
Az ilyen sémával felírt kódolást blokk-kódolásnak nevezzük, azaz blokk-kódról beszélünk akkor, ha minden egyes m hosszúságú közleményszóhoz hozzárendelünk egy és csakis egy n hosszúságú ($m \leqq n$) kódszót s ezt a hozzárendelési sémát egy blokkban írjuk le.

A kódolás célját úgy fogalmazhatjuk meg, hogy a $K \circ T \circ D$ összetett függvény (a $\circ$ jel a balösszetétel jele) nagy valószínűséggel az identitásfüggvény legyen, azaz tetszőleges $\varepsilon > 0$ esetén

$$P(K \circ T \circ D = 1Z) = 1 - \varepsilon$$

álljon fenn, ahol K és D a definícióban szereplő leképezések T a csatorna zajából származó zajfüggvény és $1Z$ pedig a Z halmaz identitásfüggvénye [2].

Egy csatornát zajosnak nevezünk, ha a közlemények a csatornán torzulást szenvedhetnek. Legegyszerűbb zajos csatorna a bináris szimmetrikus csatorna. Ekkor mind a kibocsátott, mind a vett jelek a $\{0, 1\}$ halmaz elemei; továbbá annak a valószínűsége, hogy a vett jel hibátlan p, és $q = 1 - p$ annak a valószínűsége, hogy a vett jel hibás; végül a csatornában előforduló hibák függetlenek. A bináris szimmetrikus csatornát a következő gráffal szemléltetjük:



Annak valószínűsége, hogy egy bináris szimmetrikus csatornán n jegyű vett jelsorozatban k jegy hibás a binomiális eloszlás valószínűségével egyező, azaz

$$P_k = \binom{n}{k} p^{n-k} \cdot q^k.$$

A kódolás céljának megvalósítása érdekében háromféle kódolási eljárást különböztethetünk meg:

1. *hibajelző,*
2. *hibajavító* és
3. *hibajelző és javító* kódok [3].

E dolgozat keretén belül ezek részletes tárgyalására nem térünk ki, csupán a csoportkódokkal kapcsolatosan foglalkozunk a hibajelző és javító kódok előállításának feltételeivel.

Csoportkódok

A hibajelző és hibajavító kódok közül különös jelentőséggel bírnak a csoportkódok. A csoportkódok hibajelző, illetve hibajavító képességére, a csoportkódok előállítására ugyanis egyszerű tételek fogalmazhatók meg.

Definíció. *Az olyan blokk-kódokat, melyeknek kódszavai additív csoportot alkotnak, csoportkódoknak nevezzük.*

Ezekután az alábbiakban összefoglaljuk azokat a fogalmakat és tételeket, melyek alapján a bináris csoportkódok hibajelző és hibajavító tulajdonságaira következtethetünk. Majd számítógépes előállításukra térünk ki.

Legyenek **a** és **b** kódszavak, melyek számjegyei $(a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n)$ a $\{0, 1\}$ halmaz elemei. Az **a** kódszó súlyán a benne szereplő 1-ek számát értjük, és jelöljük $s(\mathbf{a})$-val. Az **a** és **b** kódszavak távolságán pedig a kizáró—vagy összegük súlyát értjük, és jelöljük $d(\mathbf{a}, \mathbf{b})$-vel, azaz

$$d(\mathbf{a}, \mathbf{b}) = s(\mathbf{a}+\mathbf{b}).$$

Ezekután

1. Tétel. *Az összes k vagy kevesebb hiba jelzéséhez szükséges és elegendő, hogy a kódszavak közti minimális távolság legalább* $k+1$ *legyen:* minden **a**, **b** kódszavakra

$$\min [d(\mathbf{a}, \mathbf{b})] \geqq k+1.$$

2. Tétel. *Ahhoz, hogy egy bináris kódolás kijavítsa az összes k vagy kevesebb hibát, szükséges hogy a kódszavak közti minimális távolság legalább* $2k+1$ *legyen:* minden **a**, **b** kódszavakra

$$\min [d(\mathbf{a}, \mathbf{b})] \geqq 2k+1.$$

3. Tétel. *Annak a valószínűsége, hogy bináris kódolás esetén egy n jegyű közleményt hibásan értelmezünk, k vagy kevesebb hibát javító kódolás esetén legfeljebb*

$$\binom{n}{k+1} p^{n-k-1} \cdot q^{k+1} + \ldots + \binom{n}{1} pq^{n-1} + q^n.$$

4. Tétel. Legyenek egy csoportkód kódszavai $\mathbf{b}^1, \mathbf{b}^2, \ldots, \mathbf{b}^p$, akkor *az összes szópárok távolságainak minimuma megegyezik a nemnulla kódszavak súlyainak minimumával,* azaz

$$\min [d(\mathbf{b}^i, \mathbf{b}^j)] = \min [s(\mathbf{b}^k)] \quad (i \neq j).$$

A fentiek szerint, ha egy $\mathbf{b}^1, \mathbf{b}^2, \ldots, \mathbf{b}^p$ csoportkódban $\min [s(\mathbf{b}^k)] \leqq 3$ például azt jelenti, hogy a kódolás jelzi az összes kéthibát és javítja az összes egyhibát. Így igen egyszerű feltételeket adhattunk a hibajelző és hibajavító kódok képességeire vonatkozólag.

Igen fontos a csoportkódok számítógépes előállítása. Gondoljunk csak például arra, hogy az űrkutató központok hírközlései egy űrhajó számára egyedül számítógépes kapcsolattal lehetségesek, s ezen belül nem lényegtelen a közlemények vételének megbízhatósága.

A számítógépes előállítás során — a kódolással támasztott követelményen túl — igen fontos cél a számítógép kapacitásának minél jobb kihasználása. A számítógép kapacitását is figyelembe vevő csoportkód előállítások sokrétűek. Mi e dolgozat keretén belül két előállítási módra adunk számítógépes programot, melyek legjobbnak tekinthetők a fenti szempontból: a mátrix-, és polinom-kódolásra [4].

Mátrix kódolás

A közleményszavak és a kódszavak tárolásának helyigénye csökkenthető, ha csoportkódok előállításakor a mátrixszorzást használjuk fel.

Legyen adva az **a** $(a_1, a_2, \ldots, a_m)$ közleményszó, továbbá egy $E(m, n)$ kódolási mátrix; a **b** $(b_1, b_2, \ldots, b_n)$ kódszó számjegyeinek előállítását a következőképpen definiáljuk

$$b_j = \sum_{i=1}^{m} a_i e_{ij} \quad (j = 1, \ldots, n)$$

ahol e_{ij} az E mátrix i-edik sorának j-edik eleme, továbbá mindegyik a_i és e_{ji} egy Z halmaz elemei (ha Z a $\{0, 1\}$ halmaz, akkor a bináris kódolást kapjuk) és az összeadás mod z végzendő el.

Készítsünk ezután olyan programot, mely p darab közleményszó kódszavait állítja elő az $E(m, n)$ kódolási mátrix segítségével.

A program a következő főrészekből áll:

1. az a és $E(m, n)$ beolvasása,
2. a $b=a\times E$ szorzás elvégzése,
3. **b** kódjegyeinek mod z-re való redukciója és
4. **b** kiírása.

A program felírásával kapcsolatban a következő megjegyzéseket tesszük:

A WANG—2200/C számítógép előnye, hogy rendelkezik olyan hardware egységgel, mely segítségével a mátrix műveletek közvetlenül programozhatók, így a mátrix műveletek elvégzésére szolgáló programrészletek igen egyszerű struktúrájúakká válnak. Jelen programban a fent említettek közül a

MATINPUT utasítást, mátrix beolvasásra,
MATREDIM utasítást, mátrix dimenzionálásra,
MAT utasítást, mátrix szorzásra

használjuk fel.

Hátrányként jelentkezik az a tény, hogy a WANG—2200/C számítógépen a dimenzionált elemek száma egy tömb esetén maximálisan csak 255 lehet, így a közlemény és kódjegyek száma 15-nél nem lehet több. Ez a korlátozás programunk első sorában fejeződik ki csak, ettől eltekintve általánosítható részeket tartalmaz [5].

```
100 REM MATRIX KODOLAS
110 DIM A(15,15),E(15,15),B(15,15)
120 REM DIMENZIOK,SZAMRENDSZER BEOLVASASA
130 PRINT „INPUT P,M,N,Z":INPUT P,M,N,Z
140 MAT REDIM A(P,M):MAT REDIM E(M,N):MAT REDIM B(P,N)
150 REM A KOZLEMENYSZAVAK BEOLVASASA
160 PRINT „INPUT KOZLEMENY SZAVAK"
170 MAT INPUT A
180 REM A KODOLASI MATRIX BEOLVASASA
190 PRINT "INPUT KODOLASI MATRIX"
200 MAT INPUT E
210 REM A KODSZAVAK ELOALLITASA
220 MAT B=A+E
230 REM REDUKCIO MOD Z-RE
240 FOR I=1 TO P:FOR J=1 TO N
250 IF B(I,J)<Z THEN 140
260 B(I,J)=B(I,J)-Z
270 GOTO 110
280 NEXT J:NEXT I
290 REM A KODOLAS KIIRASA
300 FOR I=1 TO P
310 FOR J=1 TO M
320 PRINT A(I,J),
330 NEXT J:PRINT "→",
340 FOR J=1 TO N
350 PRINT B(I,J),
```

```
360 NEXT J:PRINT :NEXT I
370 END
```

Megjegyezzük még, hogy bármely olyan $E(m, n)$ kódolási mátrixra, amelynek az egyik (n, m) típusú részmátrixa az egységmátrix, a $\mathbf{b}=\mathbf{a}\times E$ kódolás egy monomorfizmus a közleményszavak additív csoportjából a kódszavak additív csoportjába [1].

Polinom kódolás

A csoportkódok egy speciális osztályát jelentik a polinomkódok. *Polinomkódok olyan (m, n) kódok, melyek m-jegyű közleményszavakat polinomszorzással alakítanak át n-jegyű kódszavakká.*

Legyen adva az $\mathbf{a}$ $(a_1, a_2, \ldots, a_m)$ közleményszó $(a_i \in Z)$, alkossuk meg a közleményjegyek által meghatározott

$$a(x) = a_1 + a_2x + a_3x^2 + \ldots + a_mx^{m-1}$$

$(m-1)$-edfokú polinomot. Ekkor kölcsönös egyértelmű hozzárendelést adhatunk meg a közleményszavak és a közleményjegyek által meghatározott polinomok között:

$$\mathbf{a} \rightarrow a(x).$$

Legyen továbbá adva egy k-adfokú polinom

$$g(x) = g_1 + g_2x + g_3x^2 + \ldots + g_{k+1}x^k \quad (g_1 \neq 0,\ g_{k+1} \neq 0)$$

(ahol g_i $(i=1, \ldots, (k+1)$ ugyanazon z alapú számrendszer számjegyeiből állnak, mint a_j $(j=1, \ldots, m)$ közleményjegyek), ezek után rendeljük hozzá az a közleményszóhoz azt a b $(b_1, b_2, \ldots, b_n)$ $(n=m+k)$ kódszót, melyre

$$b(x) = b_1 + b_2x + b_3x^2 + \ldots + b_nx^{n-1} = a(x)g(x)$$

ekkor mindegyik b_t $(t=1, \ldots, n)$ is a Z halmaz eleme, ha a polinomszorzás során fellépő összeadást most is mod z-re végezzük el.

Az ily módon definiált bijekciók

$$\mathbf{a} \rightarrow a(x)$$
$$a(x)g(x) = b(x)$$
$$b(x) \rightarrow \mathbf{b}$$

által meghatározott $(m, m+k)$ kódot *polinomkódnak* nevezzük.

Megjegyezzük, hogy a $g_1 \neq 0$ és a $g_{k+1} \neq 0$ feltételek az első és utolsó kódjegyek hasznosítására szolgálnak (ellenkező esetben az első, illetve utolsó kódjegyek mind csupa zérusok, így semmiféle információt nem nyújtanak).

A hibajelzés és javítás szempontjából megemlítjük a következő tételt.

Tétel. *Ha a $g(x)$ generálópolinom nem osztója egyik $1+x^t$ $(t<m+k=n)$ alakú polinomnak sem, akkor a kódszavak közti minimális távolság legalább* 3.

Az ilyen polinomok által generált kód tehát legalább kéthiba jelző és egyhiba javító kód [1, 2].

Készítsünk ezután olyan programot, mely előállítja az összes m-jegyű közleményszó (számuk z^m) egy $g(x)$ (k-adfokú) polinom által generált $(m+k)$-jegyű kódszavait.

A program a következő főrészekből áll:

1. a $g(x)$ beolvasása,

2. az a közleményszó beolvasása,
3. a $b(x)=a(x)g(x)$ polinomszorzás elvégzése,
4. $b(x)$ együtthatóinak mod z-re való redukciója,
5. a b kódszó kiírása és
6. ha van még közleményszó, akkor az eljárás ismétlése 2)-től.

A felírt programhoz ugyanazokat a megjegyzéseket fűzzük, mint amelyekről a mátrix kódolás kapcsán szóltunk.

```
100 REM POLINOM KODOLAS
110 DIM A(100),G(100),B(200)
120 REM FOKSZAMOK,SZAMRENDSZER BEOLVASASA
130 PRINT "INPUT M,K,Z":INPUT M,K,Z
140 MAT REDIM A(M):MAT REDIM G(K+1):MAT REDIM B(M+K)
150 REM A GENERALO POLINOM BEOLVASASA
160 PRINT "INPUT GENERALO POLINOM"
170 MAT INPUT G
180 REM A KOZLEMENY POLINOM BEOLVASASA
190 PRINT "INPUT KOZLEMENY POLINOM"
200 MAT INPUT A
210 REM A KODOLT POLINOM ELOALLITASA
220 FOR I=1 TO M:FOR J=1 TO K+1
230 S=S+A(I)*G(J):B(I+J-1)=B(I+J-1)+S:S=0
240 NEXT J:NEXT I
250 REM REDUKCIO MOD Z-RE
260 FOR I=1 TO M+K
270 IF B(I)<Z THEN 15
280 B(I)=B(I)-Z
290 GOTO 130
300 NEXT I
310 REM A KODOLT POLINOM KIIRASA
320 PRINT "KODOLT POLINOM"
330 FOR I=1 TO M+K
340 PRINT B(I),
350 B(I)=0
360 NEXT I
370 REM A KOVETKEZO KOZLEMENY POLINOM BEOLVASASA
380 X=X+1:PRINT :PRINT
390 IF X<Z  M THEN 60
400 END
```

Hamming-kódok

R. W. HAMMING bináris kód eljárásokra bebizonyította a következő tételt.

Tétel. *Bármely* $r>1$ *egészszám esetén létezik olyan* (m, n) *kód eljárás* $(m=2^r-1-r,\ n=2^r-1)$, *amely javítja az összes egyhibákat és más hibákat nem, és nincs olyan* (m, n) *kód eljárás, mely több hibát is javítana* [2].

A kódszavak előállítására HAMMING a következő eljárást adta meg:

1. Legyen **a** $(a_1, a_2, \ldots, a_m)$ egy közleményszó és **b** $(b_1, b_2, \ldots, b_n)$ az **a**-hoz rendelt kódszó (ahol $m=2^r-1-r$, $n=2^r-1$ és mindegyik a_i $(i=1, \ldots, m)$ $0 \vee 1$).

A **b** kódszóban a

$b_1, b_2, b_4, \ldots b^{2^{r-1}}$ jegyek ellenőrzőjegyek,

a $b_3, b_5, \ldots, b^{2^{r-1}}$ jegyek pedig közleményjegyek lesznek.

2. A közleményjegyeket helyezzük el a következő módon:

$$b_3=a_1,\ b_5=a_2,\ \ldots,\ b^{2^{r-1}}=a_m.$$

(Pl. $r=3$ esetén $m=4$, $n=7$, így

$$b_3=a_1,\ b_5=a_2,\ b_6=a_3,\ b_7=a_4).$$

3. Az ellenőrzőjegyeket ($b_2 i$ ($i=0, \ldots, r-1$)) pedig válasszuk meg úgy, hogy az alábbi egyenletek — mod z-re vett összeadással — mind teljesüljenek

$$b_1+b_3+b_5+b_7+\ldots=0$$
$$b_2+b_3+b_6+b_7+\ldots=0$$
$$b_4+b_5+b_6+b_7+\ldots=0$$

(Az előző felírás kiírt része éppen az $r=3$ esethez tartozó három egyenletet adja.)

Ezen eljárással meghatározott kódszavaknak — a tétel szerint — a minimális súlya tehát 3 (kivéve a csupa nulla kódszót).

Az eljárás szemléltetésére bemutatjuk az $r=2$ esetet:

1. ha $r=2$, akkor $m=1$ és $n=3$. Így a közleményszavak $a^1(0)$ és $a^2(1)$ lesznek. A $b^1 (b_1^1, b_2^1, b_3^1)$ és $b^2 (b_1^2, b_2^2, b_3^3)$ kódszavak kódjegyei közül

b_1^1, b_2^1 és b_1^2, b_2^2 jegyek ellenőrzőjegyek,

b_3^1 és b_3^2 jegyek pedig a közleményjegyek lesznek;

2. ezek után a közleményjegyek elhelyezése:

$$b_3^1=0 \text{ és } b_3^2=1 \text{ lesz;}$$

3. az ellenőrzőjegyek a következő egyenletekből adódnak:

$$b_1^1+b_3^1=0 \quad \text{és} \quad b_1^2+b_3^2=0$$
$$b_2^1+b_3^1=0 \qquad b_2^2+b_3^2=0$$

így az (1, 3) HAMMING-kódok

$$000 \quad \text{és} \quad 111$$

lesznek [4].

A fenti eljárást alkalmazva készítsünk ezután olyan programot, mely előállítja minden $r>1$ egészszámra az (m, n) HAMMING-kódokat. Adott $r>1$ esetén maximálisan 2^m HAMMING-kódot kell előállítanunk.

A program a következő fő részeket tartalmazza:

1. $r>1$ egészszám beolvasása,
2. az **a** közleményszó beolvasása,
3. a közleményjegyek elhelyezése,
4. az ellenőrzőjegyek kiszámítása,
5. a **b** kódjegyeinek redukciója mod 2-re,
6. a **b** kódszó kiírása,
7. ha van, még közleményszó, akkor az eljárás 2)-től való ismétlése.

A felírt programhoz megjegyezzük, hogy a WANG—2200/C számítógépen a dimenzionált elemek száma maximálisan csak 255 lehet. Így teljesülni kell az

$$n = 2^r-1 \leqq 255$$

egyenlőtlenségnek, ami azt jelenti, hogy programunkkal csak az $r=2, 3, \ldots, 8$ eseteknek megfelelő HAMMING-kódok határozhatók meg. Ez a korlátozás ismét csak programunk első utasításában fejeződik ki, így ettől eltekintve teljesen általános [5].

```
100 REM HAMMING KODOK ELOALLITASA
110 DIM A(255),B(255)
120 REM R(0<R<9) BEOLVASASA
130 PRINT "INPUT R":INPUT R
140 M=2  R-1-R:N=2  R-1
150 PRINT "R=",R, "M=", M, "N=", N
160 REM A KOZLEMENYSZAVAK BEOLVASASA
170 MAT REDIM A(M):MAT REDIM B(N)
180 MAT INPUT A
190 REM A KODSZAVAK MEGHATAROZASA
200 REM KOZLEMENYJEGYEK ELHELYEZESE
210 I=R
220 FOR J=N TO 1 STEP -1
230 K=2  (I-1)
240 IF J=K THEN 270
250 B(J)=A(J-I)
260 GOTO 280
270 B(J)=0:I=I-1
280 NEXT J
290 REM ELLENORZOJEGYEK ELHELYEZESE
300 FOR I=1 TO R
310 J=2  (I-1)
320 FOR K=J TO N STEP 2*J
330 FOR L=K TO K+J-1
340 T=T+B(L)
350 NEXT L
360 S=S+T:NEXT K
370 B(J)=S:S=0:NEXT I
380 REM REDUKCIO MOD 2-RE
390 FÜR I= 1T Ü N
400 IF B(I)<2 THEN 430
410 B(I)=B(I)-2
420 GOTO 400
430 NEXT I
440 REM A KODSZAVAK KIIRASA
450 FOR I=1 TO M
460 PRINT A(1),
470 NEXT I:PRINT "→",
480 FOR I=1 TO N
490 PRINT B(1),
500 B(I)=0
510 NEXT I
520 REM A KOVETKEZO KOZLEMENYSZO BEOLVASASA
530 Z=Z+1
540 PRINT :PRINT
550 IF Z=2  M THEN 570
560 GOTO 180
570 END
```

Megjegyezzük, hogy a HAMMING-kódok esetén a hiba felderítése a következő módon történik:

1. a kapott közlemény jegyeit helyettesítsük be a 3. alatt felsorolt $n-m$ darab egyenletbe, s ha az i-edik egyenlet teljesül a kapott közleményre, legyen $s_i=0$, különben $s_i=1$;

2. alkossuk meg az

$$s=s_{m-n}\ldots s_2s_1$$

bináris számot. Az s szám tízesszámrendszerbeli alakja legyen $\bar{s}$, akkor a $\bar{s}$-adik helyen volt hibás a közlemény.

Megemlítjük még, hogy minden HAMMING-kódolás és minden polinom kódolás helyettesíthető — alkalmas mátrixszal — mátrix kódolással.

Általános értelemben HAMMING-kódoknak neveznek minden olyan (m, n) kódot, amely az ismertetett HAMMING-eljárással készül, de nem szükségképpen teljesíti az $m=2^r-1-r$ és $n=2^r-1$ feltételeket. A HAMMING-kódok előállítására adott programunk ilyen irányba is egyszerűen általánosítható.

IRODALOM

[1] ABRAMSON, N.: Information Theory and Coding. McGraw-Hill, 1965.

[2] BIRKHOFF, G.—BARTEE, T. C.: A modern algebra a számítógéptudományban. Műszaki Könyvkiadó, Budapest, 1974.

[3] PUSKÁS—SZENDREI—SZERÉNYI: A matematika modern alkalmazásai. Tankönyvkiadó, Budapest, 1970.

[4] REZA, F. H.: Bevezetés az információelméletbe. Műszaki Könyvkiadó, Budapest, 1966.

[5] WANG-BASIC language, Reference manual, WANG Laboratories, Inc., 1975.

HERSTELLUNG VON GRUPPEN-CODES AM RECHNER WANG—2200/C

Albert Puskás

Die Arbeit befasst sich mit dem Begriff und den Eigenschaften der Gruppen-Codes, mit der Herstellung der Code-Wörter am Rechenapparat.

Besondere Bedeutung bei der Herstellung von Code-Wörtern kommt den Matritzen-Codes und den Polynom-Codes zu. Die Studie gibt diese beiden Verfahren bekannt und gibt ihr Rechner-Programm für die Rechenmaschine WANG—2200/C an. Von den binaren Gruppen-Codes sind besonders die Hamming-Codes sehr bedeutsam, deshalb teilt die Arbeit deren Rechner-Programm mit.

Die Publikation der Arbeit ist einerseits dadurch indiziert, dass als eines der wichtigsten Gebiete der Informationstheorie — die auch an sich einen höchst modernen Wissenschaftszweig darstellt — die Codierungstheorie gilt und andererseits innerhalb der Codienengstheorieim Falle geräuschvoller symmetrischer Kanäle die Gruppen-Codes eine bedeutende Rolle erfüllen. Abschliessend ist erwähnt, dass sich mit dem in der Studie erwähnten Thema auch Spezial-Kollegien befassen, so dass ihre Veröffentlichung auch didaktische Gesichtspunkte angebracht erchienen lassen.

ПОЛУЧЕНИЕ ГРУППОВЫХ КОДОВ НА ВЫЧИСЛИТЕЛЬНОЙ МАШИНЕ WANG—2200/C

А. Пушкаш

Работа занимается вопросами понятия групповых кодов, их особенностями и получением кодовых слов на вычислительной машине.

При получении кодовых слов имеют особое значение матричные и полиномные коды. Работа знакомит читателя с этими двумя методами и дает их программу для вычислительной машины типа WANG-2200/C. Из бинарных групповых кодов наиболее значительны коги Hamming, поэтому в работе дается их программа для вычислительной машины.

Публикация статьи обоснована, с одной стороны, тем, что теория информации, которая сама по себе является весьма современной областью науки, считает одной из важнейших своих отраслей теорию кодирования; с другой стороны, в рамках теории кодирования, в случае шумных симметрических каналов, групповые коды играют значительную роль. В заключение в статье отмечается, что над данной темой работы мы занимаемся и в рамках спецкурса, таким образом, публикация ее обоснована и с дидактических точек зрения.